Self Organizing Networks

WLAN IEEE 802.11 aka Wi-Fi

SS 2022 Electronic lecture

Max Riegel

SS2021 Lectures overview

- **June 2nd**
  - Wi-Fi applications and markets
  - Wi-Fi Spectrum
  - Wireless channel characteristics
  - Direct Sequence Spread Spectrum (initial Wi-Fi radio)
  - Orthogonal Frequency Division Multiplex
- **June 16th**
  - Wi-Fi 2 .. Wi-Fi 7 radios
  - Wi-Fi Standardization environment
- **June 23rd**
  - IEEE 802.11 architecture
  - Medium access functions
  - System management
- **June 30th**
  - MAC layer management
  - MAC layer frame formats
  - Quality of Service
- **July 7th**
  - Wi-Fi security
  - Mobility enhancements

WLAN IEEE 802.11 aka Wi-Fi

STANDARD REFERENCE

IEEE Std 802.11™-2020 + amendment 802.11ax™-2021

- *Can be downloaded at no charge through the IEEE Get Program*
  - *https://ieeexplore.ieee.org/browse/standards/get-program/page/series?id=68*
- *No all the features specified in the standard are available in real Wi-Fi products*
- *This lecture presents behavior of real Wi-Fi products as specified by Wi-Fi Alliance in its certification programs*
  - *https://www.wi-fi.org/discover-wi-fi/specifications*

IEEE Standard for Information technology

Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

- Revision of IEEE Std 802.11-2016
  - Revision of IEEE Std 802.11-2012
    - Revision of IEEE Std 802.11-2007
      - Revision of IEEE Std 802.11-1999
        - First IEEE 802.11 standard release in 1997
- Comprises initial IEEE Std 802.11-1999 and all amendments IEEE 802.11a-1999 … IEEE 802.11aq-2018
  - *i.e.:* a, b, d, e, g, h, I, j, k, n, p, r, s, u, v, w, y, z, aa, ac, ad, ae, af, ah, ai, aj, ak, aq

Amendment standard IEEE Std 802.11ax-2021

- Amendment 1: Enhancements for High-Efficiency WLAN

WLAN IEEE 802.11 aka Wi-Fi

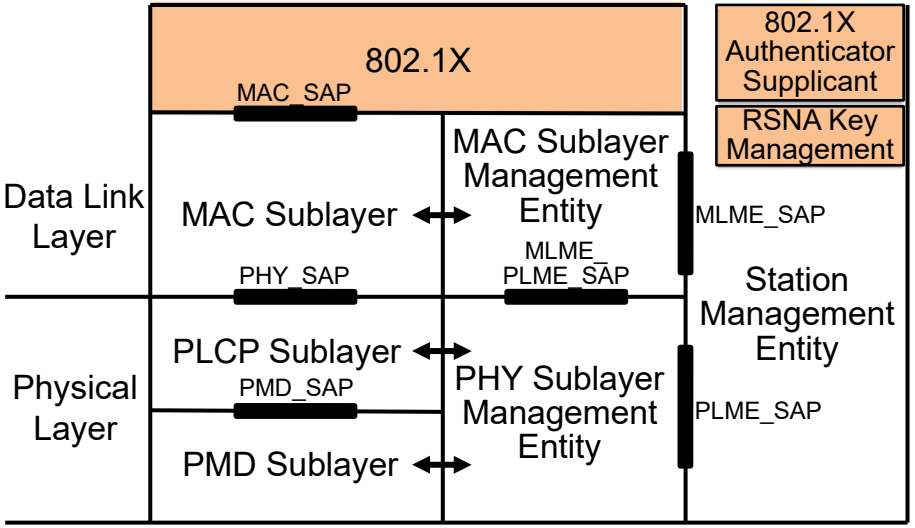
WI-FI SECURITY

Wi-Fi Security

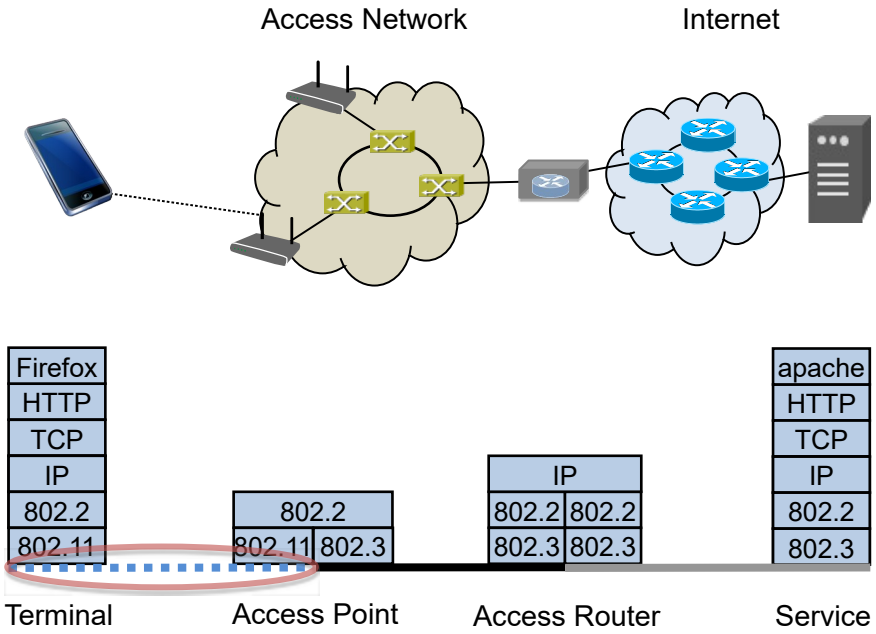
- Scope and evolution
- Robust security network
  - Configuration
  - PSK/SAE Authentication
  - IEEE 802.1X Authentication
  - Key management
  - Data protection
  - Protected management frames
  - WPA3 operational enhancements
  - Summary
- Mobility enhancements through Fast BSS Transition

IEEE802.11 Protocol architecture

- 802.1X
  - Port Access Entity
  - Authenticator/Supplicant
- RSNA Key Management
  - Generation of Pair-wise and Group Keys
- Station Management Entity (SME)
  - interacts with both MAC and PHY Management
- MAC Sublayer Management Entity (MLME)
  - synchronization
  - power management
  - scanning
  - authentication
  - association
  - MAC configuration and monitoring
- MAC Sublayer
  - basic access mechanism
  - fragmentation
  - encryption
- PHY Sublayer Management Entity (PLME)
  - channel tuning
  - PHY configuration and monitoring
- Physical Sublayer Convergence Protocol (PLCP)
  - PHY-specific, supports common PHY SAP
  - provides Clear Channel Assessment signal (carrier sense)
- Physical Medium Dependent Sublayer (PMD)
  - modulation and encoding

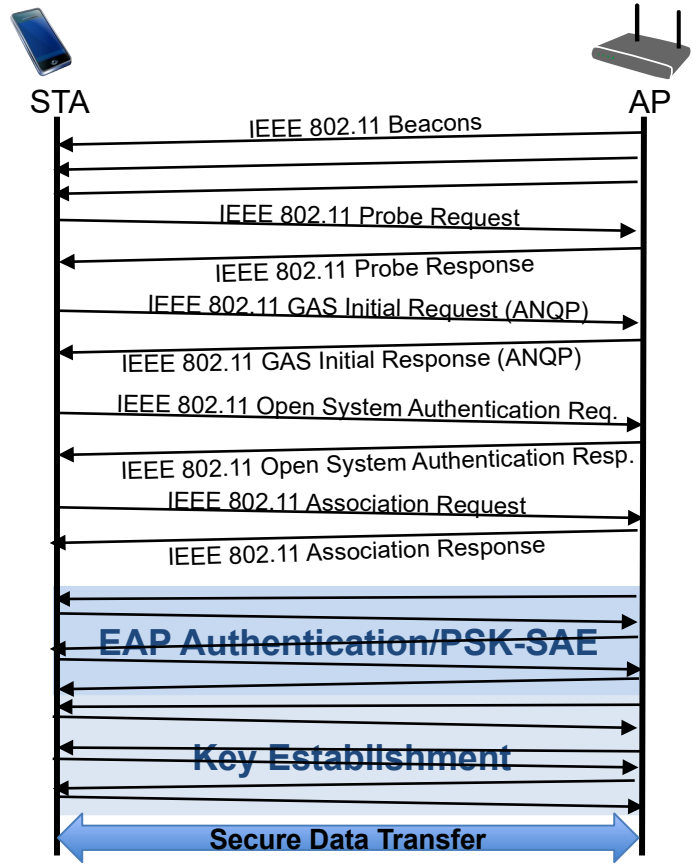


Wi-Fi/IEEE 802.11 Security



- Wireless portion of the network link is completely open to sniffing and injection if not protected.
- Wi-Fi/IEEE 802.11 security addresses authentication, confidentiality and replay protection.
  - Various methods supported.
- Ciphering works on both unicast and multicast messages

IEEE 802.11 Security Establishment



- Scanning
  - Beacon
  - Probe Request/Response
- Network Selection
  - GAS (ANQP Request/Response)
- Authentication
  - Open System Authentication
- Association
  - Association Request/Response
- Authentication/Authorization
  - Either: IEEE 802.1X EAPoL for enterprise networks
    - Starts with controlled port blocked and uncontrolled port used for exchange of authentication messages
    - EAP protocol carries authentication method
  - Or: Pre-Shared Keys for small and residential networks
    - SAE to generate fresh pairwise master keys for each session
  - Authorization comprises configuration of data path and master key delivery to AP
- Key establishment
  - Four-way handshake for establishment of pair-wise transient keys and groups keys for broad-/multicasts
- Secure data transfer
  - Secure data transfer over controlled port commence once encryption keys are established

History of Wi-Fi/IEEE 802.11 security

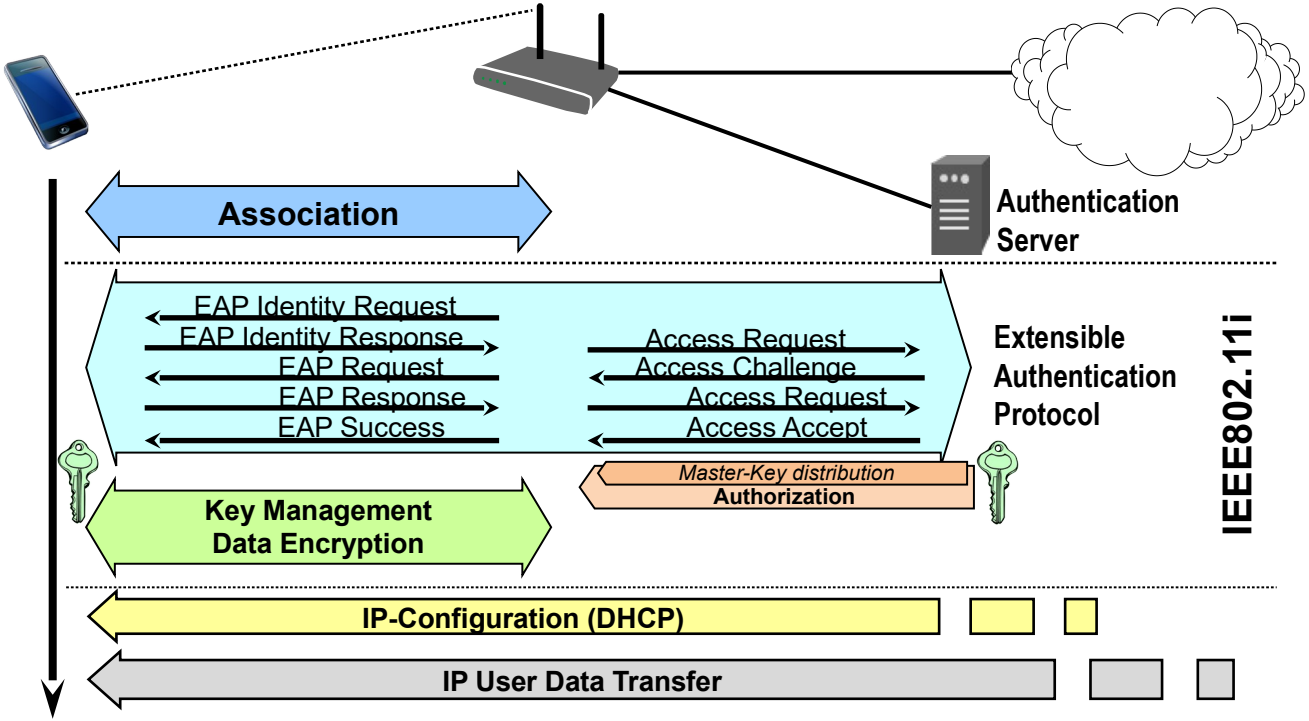
- Initial goal of IEEE 802.11 security was to provide “Wired Equivalent Privacy”
  - Usable worldwide as there was strict export regulation at that time for any ‘strong’ security with more than 40bits keys
  - IEEE 802.11-1997 provided shared key authentication based on WEP privacy mechanism
    - RC4 algorithm with 40 bit secret key
  - WEP was completely insufficient
    - WEP unsecure by design, no user authentication, no mutual authentication, missing key management protocol
- IEEE 802.11i-2004 fixed weak security by “Robust Security Network” (RSN)
  - Transitional solution w/ TKIP for fixing bugs in existing hardware
  - Conclusive solution w/ CCMP (AES) for new hardware
    - Meanwhile mainly known through WFA terms WPA (TKIP), WPA2 (CCMP), WPA3 (CCMP, GCMP)
- WPA2 supported by all Wi-Fi hardware since about 2005
  - Updated in 2018 through WPA3 for increased security and operational reliability

WLAN IEEE 802.11 aka Wi-Fi

ROBUST SECURITY NETWORK

IEEE 802.11 Robust Security Network (RSN)

RSN was introduced by IEEE 802.11i-2004



Robust Security Network Components

- Establishes Robust Security Network Associations (RSNAs)
- Comprises:
  - Configuration
  - PSK-SAE / IEEE 802.1X authentication
  - Pre-shared keys / Key distribution by RADIUS
  - Key management
  - Data protection
    - CCMP (CTR/CBC-MAC Protocol)
      - Counter mode/Cipher Block Chaining Message Authentication Code of AES
      - Achieves both confidentiality and integrity
- Amendment to RSN
  - Protected Management Frames

RSNA establishment

WPA2/3-Personal	WPA2/3-Enterprise
RSN Capability identification from Beacon or Probe Response frames	
Open System authentication.	
Cipher suite negotiation during the association process	
Case of STA and AP supporting	
PSK/SAE	802.1X Authentication
Derive Pairwise Master Key from Pre-Shared Key	IEEE Std 802.1X-2004 Authentication Derive Pairwise Master Key
Establish temporal keys by executing 4-way key management algorithm for pairwise keys and group key management for broadcast keys	
Protect the data link by operation of ciphering and message authentication with keys generated above.	
If Protected Management Frame (PMF) is enabled, the temporal keys and pairwise cipher suite is used for protection of individually addressed robust management frames	

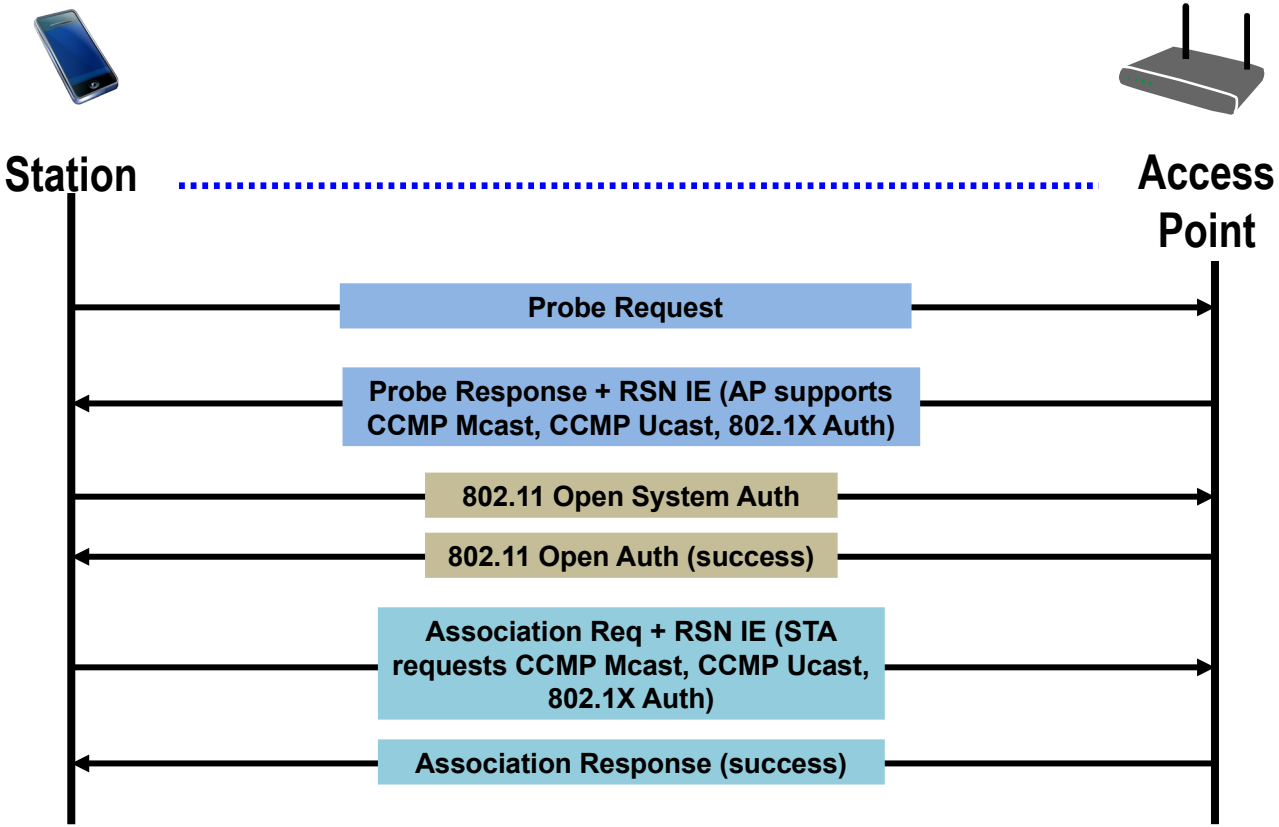
Robust Security Network

CONFIGURATION

Configuration

- Security requires networks with “right” characteristics
- AP advertises capabilities in Beacon, Probe Response
  - SSID in Beacon, Probe provides hint for right authentication credentials
  - RSN Information Element advertises all enabled authentication suites, all enabled unicast cipher suites and multicast cipher suites
- At the end of network discovery STA knows
  - SSID of the network
  - Authentication and cipher suites of the network
  - The preferred choice of authentication and cipher suites
- STA selects authentication suite and unicast cipher suite in Association Request. When AP confirms authentication and cipher suite through Association Response:
  - STA and AP have an established link for exchanging user data
  - STA and AP authenticate each other through PSK-SAE or IEEE 802.1X EAPoL

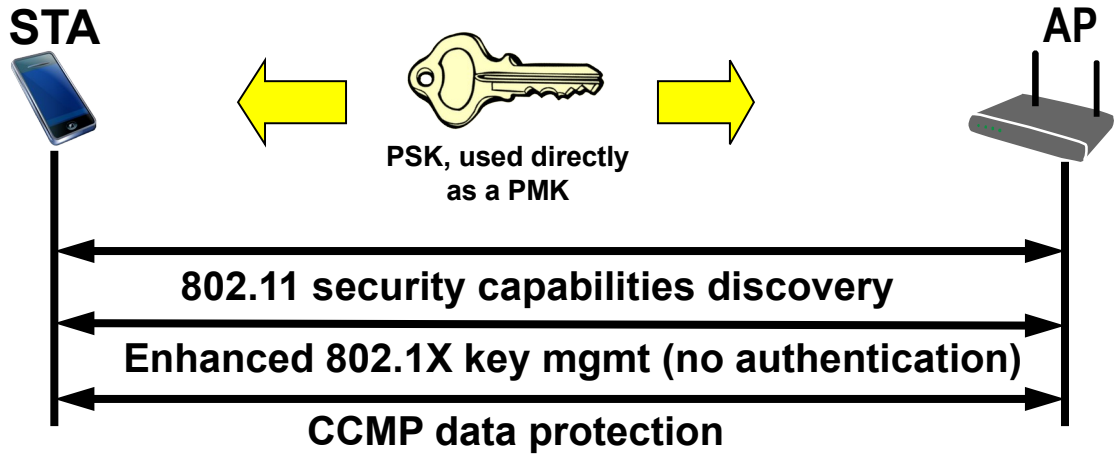
Configuration process



Robust Security Network

PSK-SAE AUTHENTICATION (WPA2/3-PERSONAL)

Legacy PSK Authentication (WPA2-Personal)

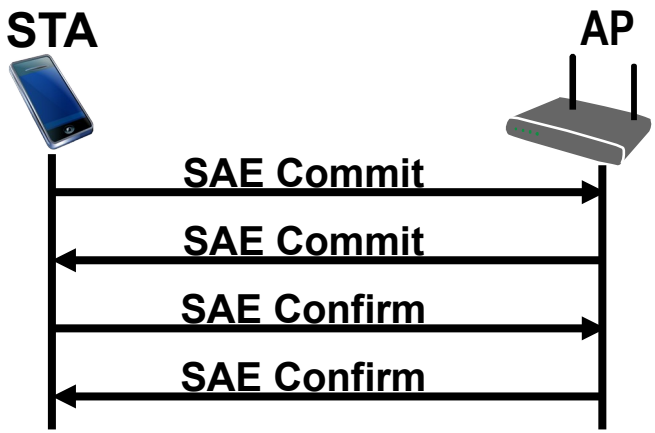


- Password-to-Key Mapping
  - Uses PKCS #5 v2.0 PBKDF2 (RFC2898; Public Key Cryptography Specification #5 v2.0, Password Based Key Derivation Function #2), to generate a 256-bit PSK from an ASCII password
  - Quality of PSK depends on quality of ASCII password!
- Reason to provide PSK-Mode:
  - Home users might configure passwords, but will never configure keys

WPA3-Personal deploys SAE for key generation

- Replacement of legacy PSK password-to-key mapping through Simultaneous Authentication of Equals (SAE)
  - SAE has been made available in IEEE 802.11 through IEEE 802.11s amendment for authentication and encryption among mesh partners.
  - Resistant to offline dictionary attacks to determine the network password
    - Requires repeated active attacks for each guess of the password
  - Provides forward secrecy
    - Property of secure communication protocols in which compromise of long-term keys does not compromise past session keys.
  - Retains the ease-of-use and system maintenance associated with WPA2-Personal
- WPA3-Personal Transition Mode allows for gradual migration while maintaining interoperability with WPA2-Personal devices

Simultaneous Authentication of Equals



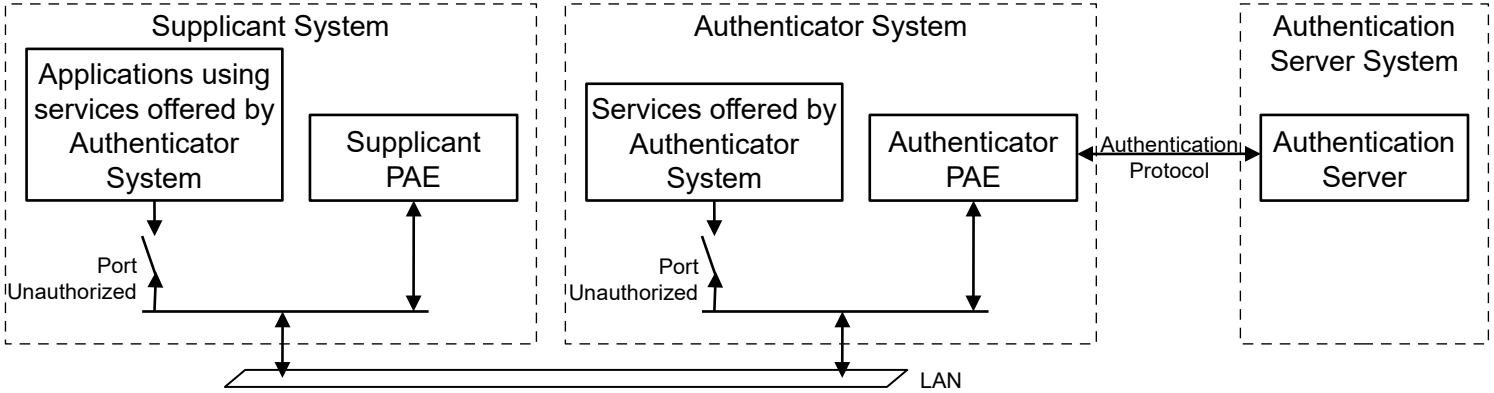
- SAE is based on a Dragonfly handshake as defined in RFC 7664
- Authenticates two peers using only a password, resulting in a shared secret between the two peers that can subsequently be used for secret communication.
- The SAE handshake negotiates a fresh Pairwise Master Key (PMK) per client, which is then used in a traditional Wi-Fi four-way handshake to generate session keys.
- It provides a secure alternative to using certificates or when a centralized authority is not available.
- Neither the PMK nor the password credential used in the SAE exchange can be obtained by a passive attack, active attack, or offline dictionary attack.

Robust Security Network

802.1X AUTHENTICATION (WPA2/3-ENTERPRISE)

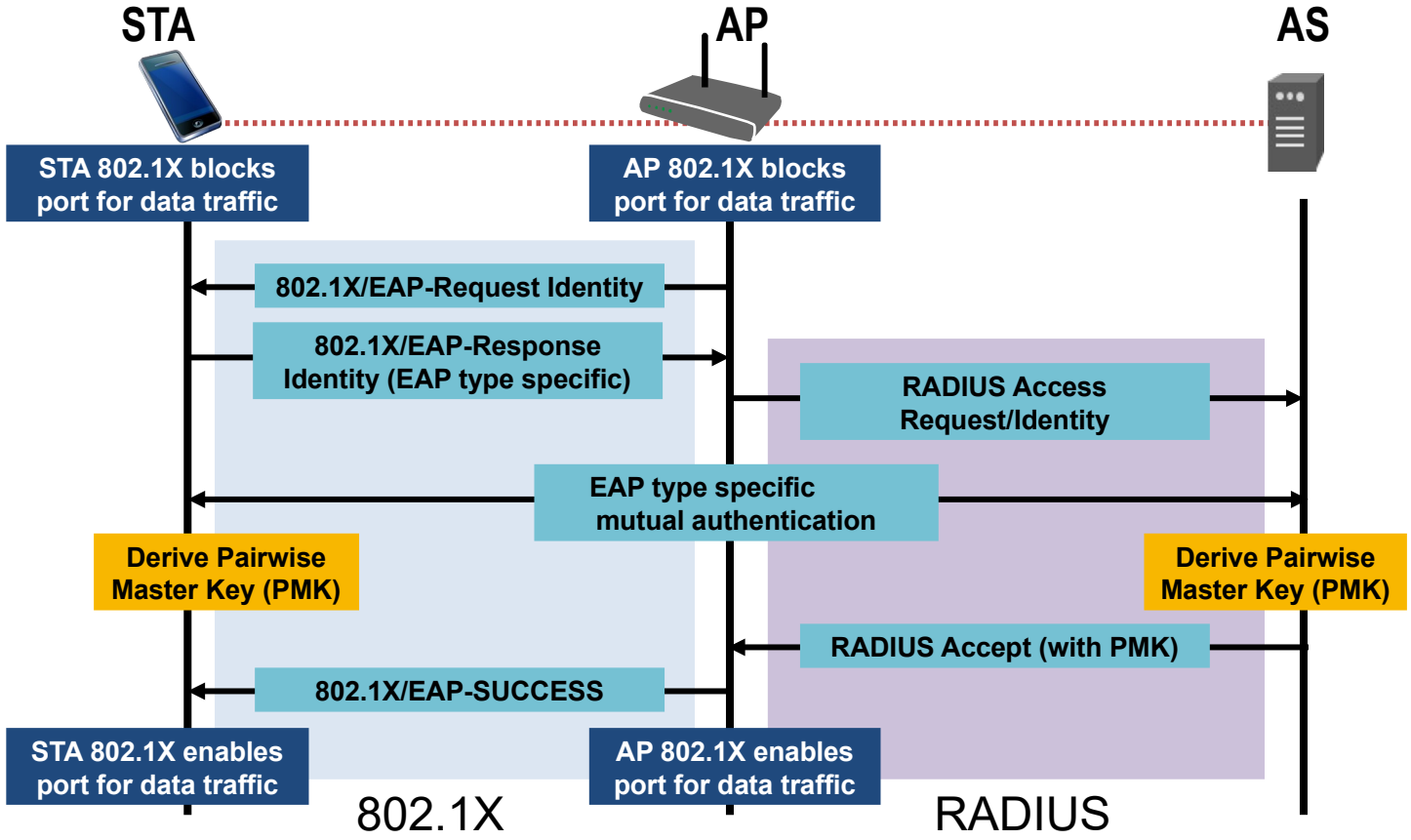
IEEE 802.1X aka EAPoL (EAP over LAN)

- Inherits EAP architecture (RFC 3748, RFC 5247)
  - "Authenticator" located in AP, "Supplicant" located in STA
  - Transport for EAP messages over IEEE 802 LANs



- Deploys Port Authentication Entity (PAE) with uncontrolled port and controlled port.
- IEEE 802.1X/EAP provides no cryptographic protections
  - No defense against forged EAP-Success, relies on EAP method to detect all attacks
  - "Mutual" authentication and binding must be inherited from EAP method

IEEE 802.1X Message flow



IEEE 802.1X Authentication

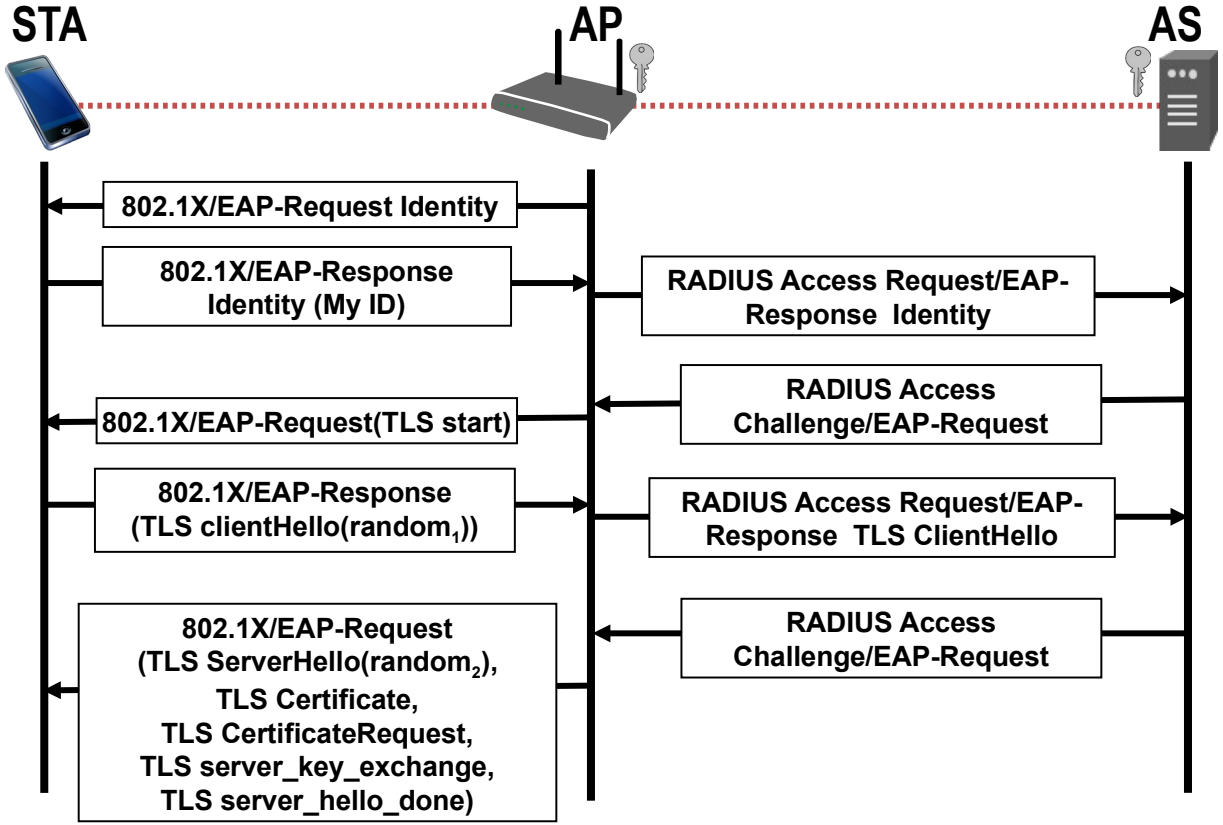
- Establishment of a mutually authenticated session key between Authentication Server (AS) and STA
  - At the begin of session ⇒ key is fresh
  - Mutually authenticated ⇒ bound only to AS and STA
- Authentication method defends against eavesdropping, man-in-the-middle attacks, forgeries, replay, dictionary attacks against either party

- At the end of authentication:
  - The AS and STA have established a session bound to a mutually authenticated Master Key
  - Delivered by EAP method
    - Authentication Server forwards PMK to the AP
- Identity protection (privacy) not provided
  - MAC addresses are not hidden
  - However, identities can protected by random MAC addresses and tunneled EAP methods

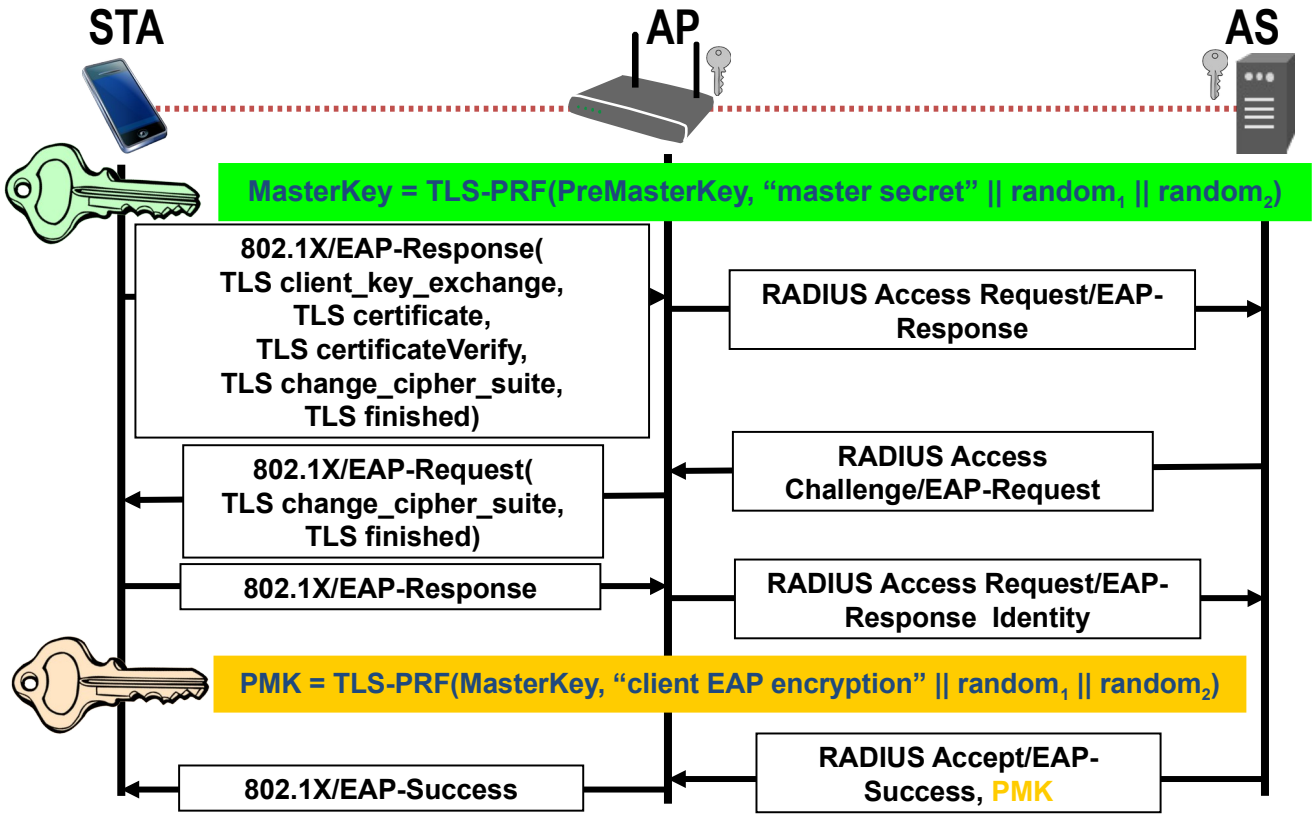
EAP Menthods, e.g. EAP-TLS

- EAP-TLS is not part of IEEE 802.11i;
  - neither is any other specific authentication method used for Wi-Fi
- But EAP-TLS has been the initial (only) solution of an EAP method for IEEE 802.11
  - Met all IEEE 802.11 requirements, while other widely deployed methods did not
- EAP-TLS = TLS Handshake over EAP
  - EAP-TLS defined by RFC 5216, TLS defined by RFC 2246
  - Must have the capability to verify the identity of the peer
    - Requires deployment of public key infrastructure
    - Mutual authentication requires X.509 certificates for both, STA and Authentication Server

802.1X Authentication with EAP-TLS (1)



802.1X Authentication with EAP-TLS (2)



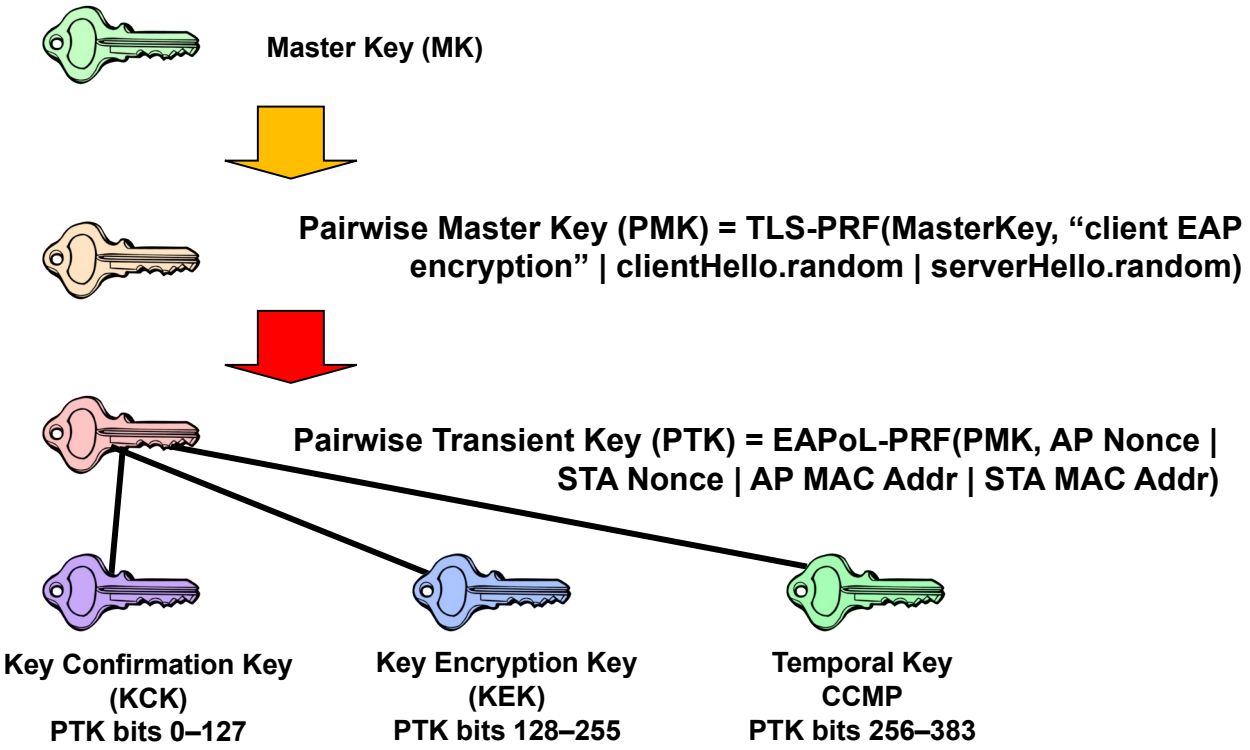
Robust Security Network

KEY MANAGEMENT

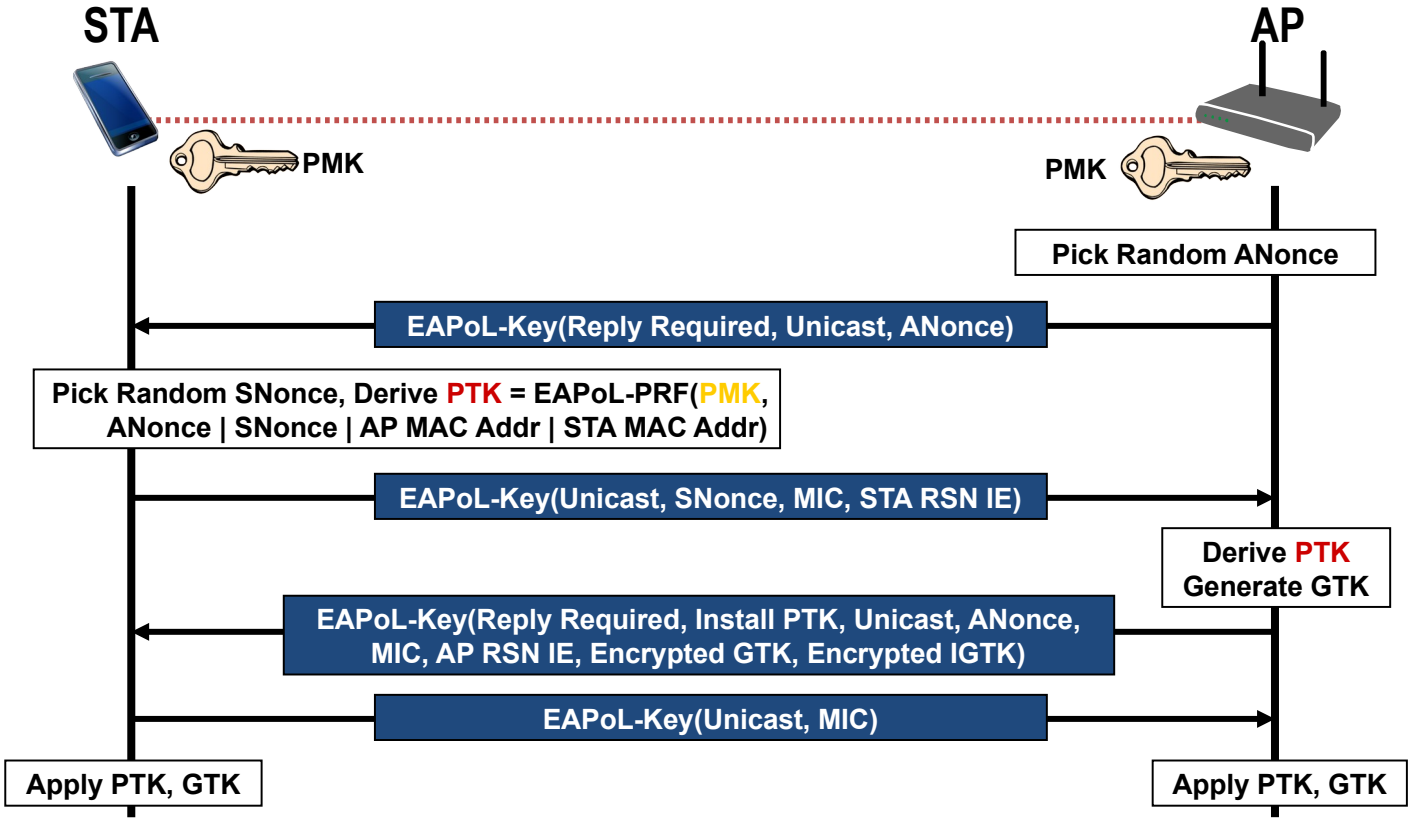
Key Management

- Redesigned by IEEE 802.11i to fix original 802.1X key management
  - Based on availability of a Pairwise Master Key (PMK)
  - AP and STA use PMK to derive Pairwise Transient Key (PTK)
  - PTK used to protect the data link
- Limitations:
  - No explicit binding to preceding association, authentication
  - Keys are only as good as back-end allows
- 4-Way Handshake
  - Establishes a fresh pairwise key bound to STA and AP for this session
  - Proves liveness of peers
  - Demonstrates there is no man-in-the-middle between PTK holders if there was no man-in-the-middle holding the PMK
  - Synchronizes pairwise key use
  - Piggybacked Group Key provisioning to STA

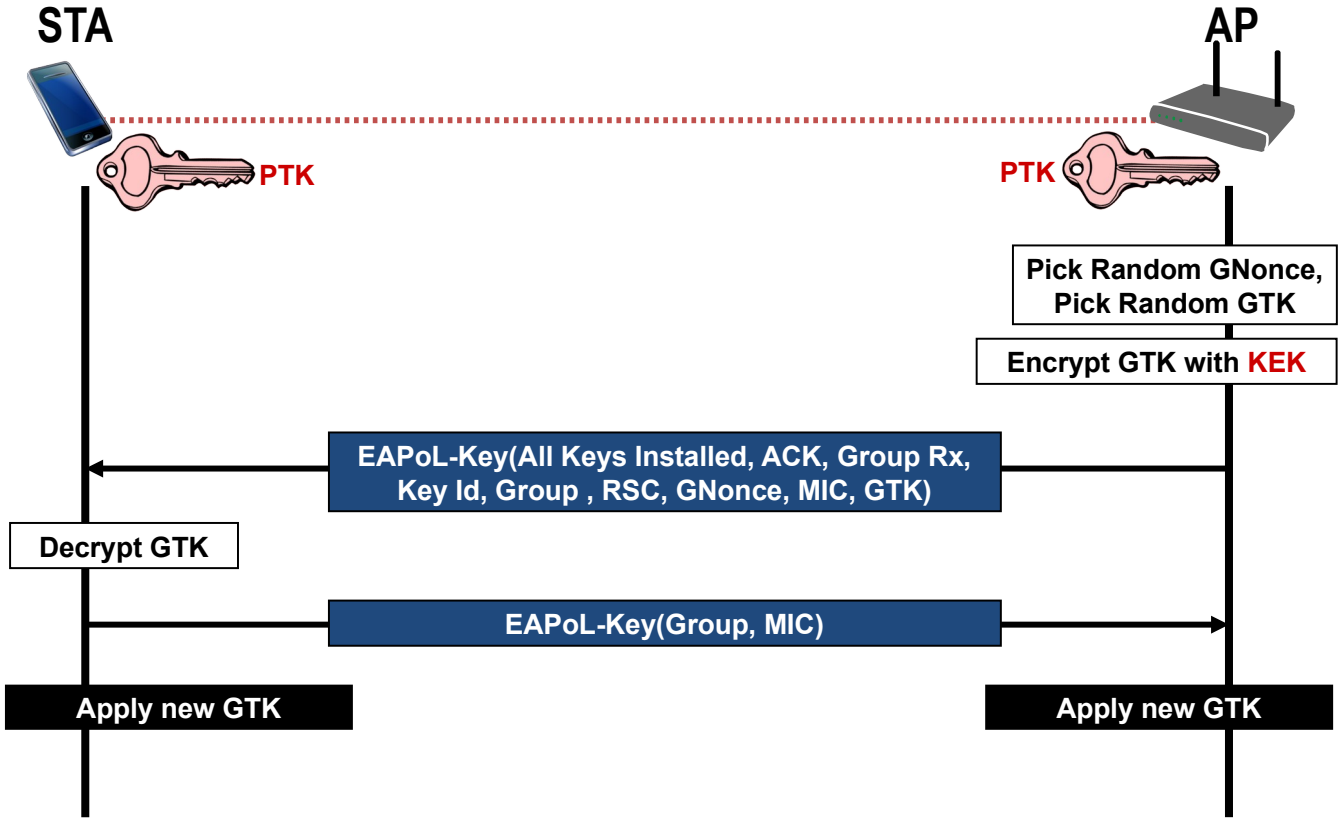
Pairwise Key Hierarchy



4-Way Handshake to establish Temporal Keys for ciphering



Optional Group Key handshake to refresh GTK



Robust Security Network

DATA PROTECTION

General data protection requirements

- Never send or receive unprotected packets
- Authenticate message origin
  - Forgeries prevention
- Sequence packets
  - Replay detection
- Avoid rekeying
  - 48 bit packet sequence number
- Protect source and destination addresses
- Use strong cryptography
  - For both, confidentiality and integrity

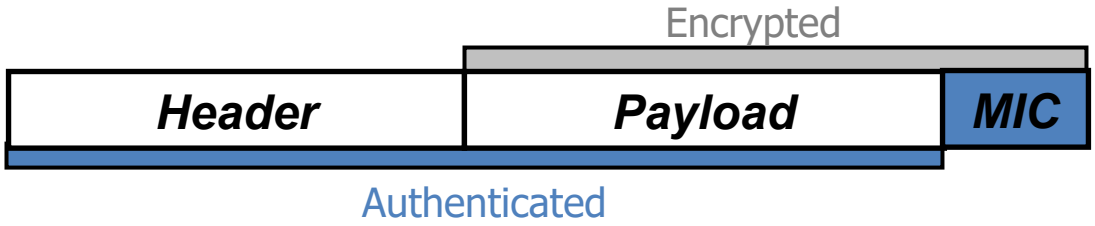
CCM provides strong cryptograph

Counter mode with Cipher-block chaining Message authentication code (CCM) is specified in IETF RFC 3610

- A symmetric key block cipher mode providing confidentiality using counter mode (CTR) and data origin authenticity using cipher-block chaining message authentication code (CBC-MAC)
  - Assumes 128 bit block cipher – IEEE 802.11i uses AES
- CCM Properties
  - CCM provides authenticity and privacy
  - CCM is packet oriented
  - CCM can leave any number of initial blocks of the plaintext unencrypted

CCMP (CTR with CBC-MAC Protocol)

- Especially designed for IEEE 802.11i
- CCMP makes use of CCM to
  - Encrypt packet data payload
  - Protect packet selected header fields from modification



- CBC-MAC used to compute a MIC on the plaintext header, length of the plaintext header, and the payload
- CTR mode used to encrypt the payload and the MIC
- Same 128-bit Temporal Key for encryption and authentication at both AP and STA
  - Generated and established through 4-way handshake

Stronger cryptography through WPA3-Enterprise

- Introduces an enhanced 192-bit security mode
- Replaces 128-bit CCMP through 256-bit GCMP (Galois/Counter Mode Protocol)
  - GCMP was introduced to IEEE 802.11 through IEEE 802.11ad (WigGig)
  - 256-bit GCMP was used instead of 192-bit GCMP because of broader adoption in industry
- In addition:
  - More secure key derivation and key confirmation through 384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (HMAC-SHA384)
  - More secure key establishment and authentication through Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) using a 384-bit elliptic curve
  - Used security algorithms are known as ‘Suite B’
- Mandatory support of Protected Management Frames required
- No need for transition mode, but considerations given for interoperability between WPA2-Enterprise and WPA3-Enterprise

Robust Security Network

PROTECTED MANAGEMENT FRAMES

Protected Management Frames (PMF)

- Management frames are used to initiate and tear down sessions
  - E.g.: authentication, de-authentication, association, dissociation, beacon, probe
- Management frames must be transmitted as open
  - To be heard and understood by all clients
- Protection necessary to avoid attacks through forgery
- IEEE 802.11w-2009 introduced Protected Management Frames (PMF) service to
  - Disassociation,
  - De-authentication, and
  - Robust Action Frames (IEEE 802.11-2020 Table 9-51).
    - I.e: Spectrum management, QoS, DLS, Block Ack, Radio measurement, Fast BSS Transition, SA Query, WNM, Mesh, Multihop, Vendor specific protected

PMF components and operation

- Integrity Group Temporal Key (IGTK)
  - Random value, assigned by the broadcast/multicast source STA/AP
    - Protection of its group addressed MAC management protocol data units (MMPDUs)
  - Key Distribution:
    - With PMF the AP includes the encrypted GTK and IGTK values in the EAPOL-Key frame
      - Message 3 of 4-way handshake.
    - For later changes of the GTK, AP sends the new GTK and IGTK to the client using the Group Key Handshake.
- Broadcast/Multicast Integrity Protocol
  - Adds a MIC calculated based on the shared IGTK key
- Operation
  - Client protection through cryptographic protection to de-authentication and dissociation frames
  - Infrastructure protection through Security Association (SA) tear down protection mechanism

Robust Security Network

WPA3 OPERATIONAL ENHANCEMENTS

WPA3 Operational Enhancements

- EAP Server Certificate Validation (SCV)
  - Mandatory for Wi-Fi CERTIFIED WPA3-Enterprise
- SAE Hash-to-Element
  - Mandatory for Wi-Fi CERTIFIED WPA3
- Transition Disable
  - Mandatory for Wi-Fi CERTIFIED WPA3
- SAE Public Key (SAE-PK)
  - Optional feature for Wi-Fi CERTIFIED WPA3
- Wi-Fi QR code
  - Optional feature for Wi-Fi CERTIFIED WPA3
- Beacon Protection
  - Optional feature for Wi-Fi CERTIFIED WPA3
- Operating Channel Validation
  - Optional feature for Wi-Fi CERTIFIED WPA3
- Privacy Extension Mechanisms
  - Optional feature for Wi-Fi CERTIFIED WPA3

Mandatory WPA3 enhancements briefly explained...

- EAP Server Certificate Validation (SCV)
  - STA must perform SCV whenever EAP-TLS, EAP-TTLS or EAP-PEAP is used
    - Ensure proper certificate validation with TLS-based WPA3-Enterprise
    - Protect against active evil-twin AP attacks on client devices
  - Allowed trust anchors are server certificate, or CA root cert, pinned to network profile, or CA in trust root store plus explicit domain name (partial or FQDN)
    - Trust-on-First-Use (TOFU), aka “UOSC”, is allowed by default
    - Operator can include Trust Override Disable (TOD) policy in server cert
    - SCV cannot be disabled (e.g. “Do not validate” option in UI is not allowed)
- SAE Hash-to-Element
  - Computationally efficient technique to mitigate side-channel attacks, based on crypto best practice (see IETF draft-irtf-cfrg-hash-to-curve)
  - Defined in IEEE 802.11-2020; AKMs remain the same (SAE and FT-SAE)
- Transition Disable
  - Provides protection against Transition mode downgrade attacks on STAs
  - When configured, AP sends Transition Disable indication to STAs at association
    - Protected in 4-way handshake
  - The STA disables the indicated Transition modes in its network profile for subsequent connections to that network (SSID)

Optional WPA3 enhancements briefly explained...

- SAE Public Key (SAE-PK)
  - Better security for “small” public networks that cannot deploy EAP authentication
    - Use cases where, today, a WPA2/WPA3-Personal password is shared on signage in a cafe/restaurant, meeting venue, etc.
    - Avoids evil-twin AP attacks by attacker who knows the password
  - Extension to SAE protocol (same AKM) through password is specially generated, embeds base32 fingerprint of public key
    - Example password: a2bc-de3f-ghi4
  - During SAE authentication, AP signs the SAE transcript, and STA validates the signature using the trusted fingerprint decoded from the password
    - Authentication fails if public key or signature not validated by STA

- Wi-Fi QR code
  - Formalized “WIFI” URI definition according https://www.iana.org/assignments/uri-schemes/prov/wifi
  - Easy way for a STA (with a camera) to connect to a new network
  - Backward-compatible with current de-facto standard WIFI URI format
  - Adds support for WPA3 features, including Transition Disable, SAE-PK, and non-ASCII passwords (percent-encoded)

Further optional WPA3 enhancements briefly explained...

- Beacon Protection
  - Provides integrity protection of Beacon frames to protect against malicious manipulation of Beacon frame content, e.g. denial-of-service “quiet” attack and WMM parameter set attack, Transmit Power Control limit attack
- Operating Channel Validation
  - Provides mutual verification between peers (e.g., AP and STA) of the current operating channel during security-related exchanges and channel switches to protect against channel-based man-in-the-middle attacks
- Privacy Extension Mechanisms
  - Consistent implementation guidelines and use cases for MAC address randomization
    - STA shall construct a uniquely randomized MAC address per SSID, unless saved Wi-Fi network profile explicitly requires to use its globally unique MAC address.
    - The STA may construct a new randomized MAC address for an SSID at its discretion.
      - During Active Scanning while not associated to a BSS
      - For each ANQP exchange while not associated to a BSS

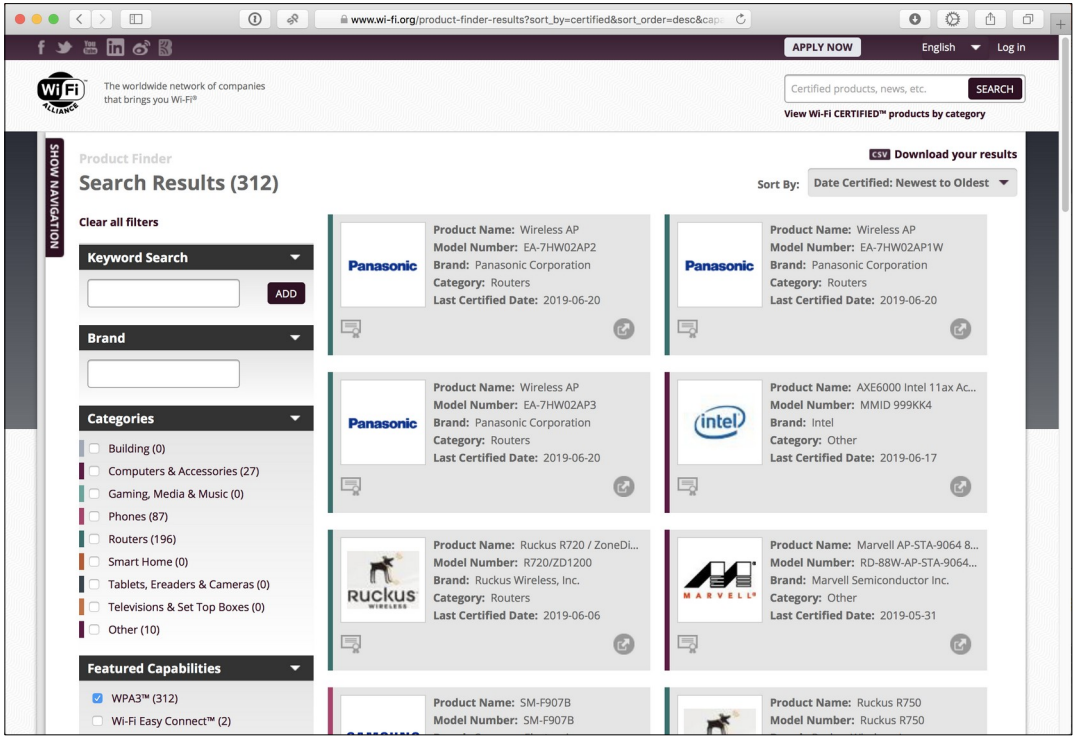
Robust Security Network

SUMMARY

Steps of Wi-Fi security establishment

- Security negotiation
  - Determine promising parties with whom to communicate
  - AP advertises network security capabilities to STAs
- Authentication based on 802.1X
  - Centralize network admission policy decisions at the Authentication Server
  - Mutually authenticate STA and Authentication Server representing AP
  - Generate Master Key as a side effect of authentication
  - Use master key to generate session keys = authorization token for access by STA
- RADIUS-based key distribution
  - Authentication Server moves (not copies) session key (PMK) to STA's AP
- Key management by 4-way handshake
  - Bind PMK to STA and AP and confirm both AP and STA possess PMK
  - Generate fresh operational keys (PTK) and communicate group keys (GTK, IGTK)
  - Prove each peer is live and synchronize PTK and GTK, IGTK use
- Data Protection
  - Encrypt data by CTR (AES)
  - Authenticate data by CBC-MAC (AES)

WPA3 product support



- https://www.wi-fi.org/product-finder-results?sort_by=certified&sort_order=desc provides overview of WPA3 certified products.

WLAN IEEE 802.11 aka Wi-Fi

MOBILITY ENHANCEMENTS THROUGH FAST BSS TRANSITION

Fast BSS Transition (FT) introduction

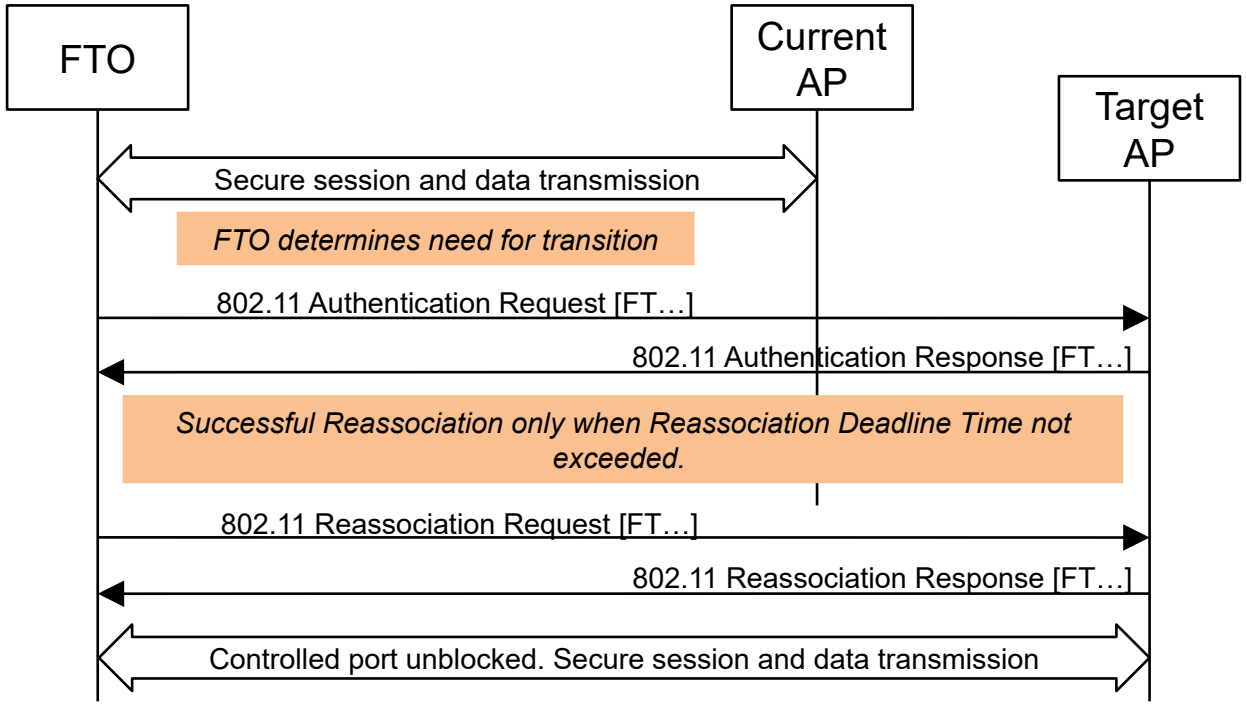
- Without FT, a BSS transition requires the following four stages:
  - 1. Scanning for target APs.
  - 2. Open 802.11 authentication.
    - Only for compatibility with the original 802.11 specification and achieves no true user authentication.
  - 3. Reassociation.
  - 4. PTK derivation and installation.
    - The complexity of this step depends on whether a new complete 802.1X reauthentication is involved in providing the PMK at the new AP.
    - At minimum, at least a four-way handshake is required to derive the PTK.
- FT completely removes need for reauthentication and succeeding 4-way handshake
  - Defining a new key hierarchy allowing for local derivation of PMK for APs of the same mobility domain.
  - Collapsing the four-way handshake into the 802.11 authentication/association exchange
- FT Information Elements
  - The Fast Transition Information Element (FTIE) enables the advertisement of network-infrastructure resource-reservation information and security-policy information.
  - The Mobility Domain Information Element (MDIE) identifies all the APs of the current mobility domain.

FT protocol overview

- FT protocol was specified through IEEE 802.11r-2008
- Protocol initiated during the initial association of FT Originator (FTO) and AP.
  - FT protocol is part of the re-association service
    - Only apply to STA transitions between APs within the same mobility domain within the same ESS.
  - Initial exchange: FT initial mobility domain association
  - Subsequent re-associations to APs within the same mobility domain may make use of the FT protocols.
- Two FT protocols are defined:
  - FT Protocol when no resource request prior to its transition.
  - FT Resource Request Protocol when a FTO has to request a resource prior to transition.
- Two FT methods:
  - Over-the-Air
  - Over-the-DS
- APs advertise both, capabilities and policies for the support of the FT protocols and methods through FTIE.

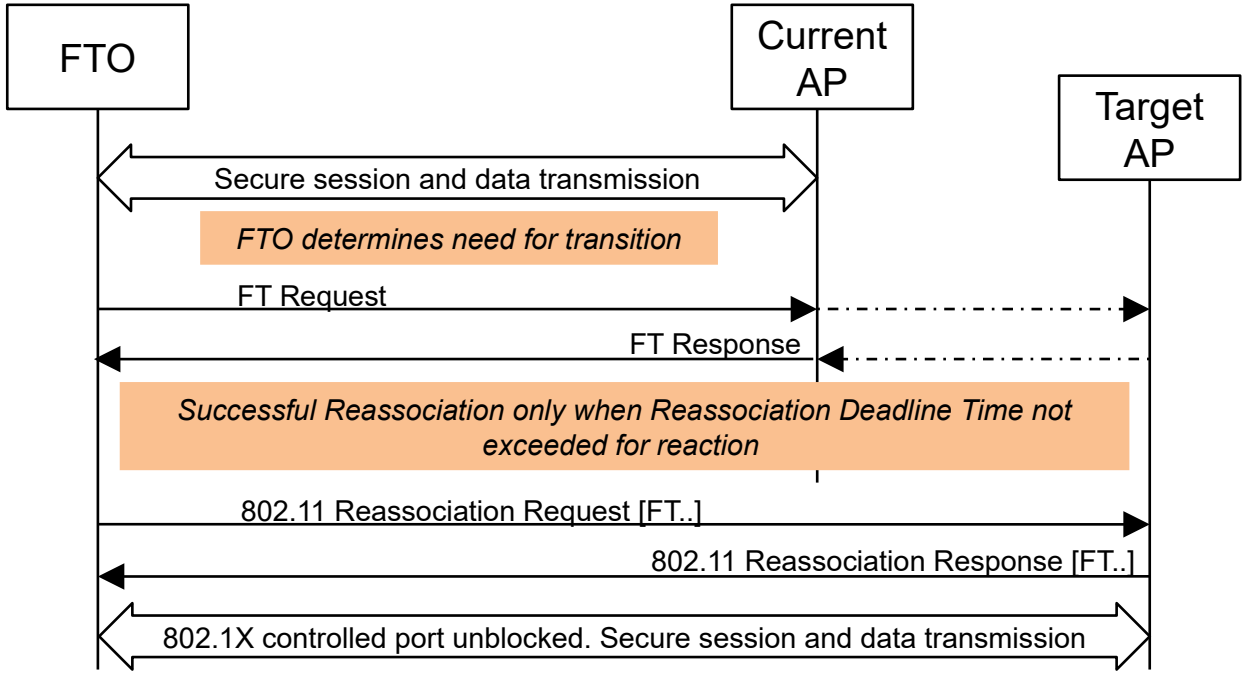
Over-the-air Fast BSS Transition

- The FTO communicates directly with the target AP
  - Use of IEEE 802.11 authentication frame with the FT authentication algorithm.



Over-the-DS Fast BSS Transition

- The FTO communicates with the target AP via the current AP.
  - The communication between the FTO and the target AP is carried in FT Action frames between the FTO and the current AP.



Questions and answers

Security questions…

1) What are the initial MAC management message exchanges before the EAPoL authentication exchange?
2) What does RSN mean?
3) What is the purpose of IEEE 802.1X?
4) Which cryptographic methods are mandatory for RSN?
5) What kind of authentication is supported by RSN?
6) Which name is used by Wi-Fi Alliance to denote the certification of latest IEEE 802.11 security?
7) Which method does WPA3-Personal use for authentication and key generation?
8) What is the difference between WPA3-Enterprise and WPA3-Personal authentication?
9) Which authentication protocols are used in the Robust Security Network?
10) What is the outcome of the configuration phase in the Robust Security Network?
11) What are the peer entities of the EAP protocol in IEEE 802.11?
12) How is the master key transferred from the AAA server to the AP?

More security questions…

13) Which peer entities do each create the PMK used for the user data encryption in WPA3-Enterprise?
14) Where is the supplicant located used in WPA3-Enterprise?
15) What is the function of the PAE in IEEE 802.1X?
16) What kind of credentials are used in EAP-TLS to identify the peers?
17) Why was the SAE method introduced in WPA3?
18) Which key is used as input to start the 4-way handshake in RSN?
19) What is the purpose of the group key in IEEE 802.11?
20) Which default key length is used in RSN for AES?
21) Why is it important that CCMP protects but does not encrypt the header part of a WLAN frame?
22) What is the purpose of Protected Management Frames?
23) What is the purpose of Fast BSS Transition?
24) How can the Fast Transition Originator communicate with the Target AP?

The End

Anything open?

Thank you very much for attending this lecture:-).